CLAIMS

We claim:

1. A method in a network access device comprising:

without proxying, analyzing each of a stream of packets traversing a single connection through the network access device from an external host to a protected host;

forwarding each allowed packet of the stream of packets as long as the connection is active; and

if one of the stream of packets is determined to be disallowed by said analyzing, then discarding the disallowed packet and terminating the connection, causing the protected host to discard those packets received on the terminated connection.

2. The method of claim 1 wherein analyzing each of the stream of packets comprises inspecting a header of each of the stream of packets against a packet filter.

3. The method of claim 1 wherein analyzing each of the stream of packets comprises inspecting a payload of each of the stream of packets for disallowed content.

4. The method of claim 3 wherein inspecting the payload of each of the stream of packets comprises copying the payload, analyzing the payload, and discarding the corresponding packet if the payload is threatening.

5. The method of claim 1 further comprising:

copying a payload from each of a plurality of packets that comprise a file, the stream of packets including the plurality of packets;

forwarding all but the last of the plurality of packets to the protected host;

reassembling the plurality of packets into the file;

analyzing the file;

if the file is a threatening file then discarding the last packet and terminating the connection; and

if the file is non-threatening, then forwarding the last packet.

6. A computer implemented method comprising:

copying a packet payload of each of a plurality of packets received on a single connection between an external host and a protected host that carries a stream of packets the stream of packets including the plurality of packets;

forwarding all but the last of the plurality of packets to the protected host;

reassembling the copied packet payloads into a file;

analyzing the file to determine if the file is allowed or disallowed;

if the file is allowed, then forwarding the last packet to the protected host; and

if the file is determined to be disallowed, then dropping the last packet and terminating the connection.

7. The computer implemented method of claim 6 wherein the analyzing the file comprises performing anti-virus analysis on the file.

8. The computer implemented method of claim 6 further comprising:

analyzing a header of each of the stream of packets; and

if one of the stream of packets is determined to be disallowed, then discarding the disallowed packet and terminating the connection.

9. The computer implemented method of claim 8 wherein analyzing the header comprises inspecting addresses indicated in the header against a packet filter.

10. The computer implemented method of claim 6 further comprising:

individually analyzing each of the copied packet payloads; and if one of the copied packet payloads is determined to be threatening, then discarding the corresponding packet and terminating the connection.

11. The computer implemented method of claim 10 wherein analyzing each of the copied packet payloads comprises inspecting each copied packet payload against a list of disallowed content and determining if each copied packet payload includes threatening script.

12. The computer implemented method of claim 6 further comprising maintaining the connection while analyzing the file.

13. The computer implemented method of claim 12 wherein maintaining the connection comprises:

decapsulating the last packet's payload;

fragmenting the last packet's payload into subparts;

encapsulating each subpart; and

forwarding each subpart until analysis is complete.

14. The computer implemented method of claim 12 wherein maintaining the connection comprises:

copying each of the plurality of packets but the last packet before forwarding each of the plurality of packets; and

holding the last packet and repeatedly forwarding the last copied packet.

15. The computer implemented method of claim 12 wherein maintaining the connection comprises increasing transmission latency of each acknowledgement transmitted from the protected host to the external host until the analysis is complete.

16. The computer implemented method of claim 6 wherein forwarding each of the plurality of packets comprises transmitting a message indicating that each of the of the plurality of packets is allowed.

17. A computer implemented method comprising:

supporting a connection from an external host to a protected host;

analyzing a header of each packet received over the connection from the external host;

terminating the connection if a first packet received over the connection is determined to be disallowed and discarding the first packet;

if the connection is not terminated, copying the first packet's payload;

analyzing the first packet's payload;

terminating the connection if said first packet's payload is determined to be disallowed and discarding the first packet;

if the connection has not been terminated and if said first packet's payload is not a last block of a file, then forwarding said first packet to the protected host;

if said first packet's payload is the last block of a file, then reassembling the first packet's payload with a set of one or more previously copied packet payloads into the file;

analyzing the file to determine if the file is allowed or disallowed;

if the file is disallowed then dropping the first packet and terminating the connection; and

if the file is allowed then forwarding the first packet.

18. The computer implemented method of claim 17 further comprising maintaining the connection while analyzing the file.

19. The computer implemented method of claim 18 wherein maintaining the connection comprises:

decapsulating the last packet's payload;

fragmenting the last packet's payload into subparts;

encapsulating each subpart; and

forwarding each subpart until analysis is complete.

20. The computer implemented method of claim 18 wherein maintaining the connection comprises:

copying each of the plurality of packets but the last packet before forwarding each of the plurality of packets; and

holding the last packet and repeatedly forwarding the last copied packet.

21. The computer implemented method of claim 18 wherein maintaining the connection comprises increasing transmission latency of each acknowledgement transmitted from the protected host to the external host until the analysis is complete.

22. The computer implemented method of claim 6 wherein the analyzing the file comprises performing anti-virus analysis on the file.

23. The computer implemented method of claim 8 wherein analyzing the header comprises inspecting addresses indicated in the header against a packet filter.

24. The computer implemented method of claim 10 wherein analyzing each of the copied packet payloads comprises inspecting each copied packet payload against a list of disallowed content and determining if each copied packet payload includes threatening script.

25. An apparatus comprising:

a forwarding module to forward packets of a datastream along a connection between a protected host and an external host; and a datastream analysis module coupled with the forwarding module, the datastream analysis module to analyze each of the packets to determine if each of the packets are allowed or disallowed and to terminate the connection upon determining one of the packets to be disallowed and to discard the disallowed packet, causing the protected host to discard packets received on the terminated connection prior to the disallowed packet.

26. The apparatus of claim 25 further comprising a memory to store each of the packets until forwarded or discarded.

27. The apparatus of claim 25 further comprising a memory coupled with the datastream analysis module, the memory to store copies of each of the packets' payloads.

28. A machine-readable medium that provides instructions, which when executed by a set of one or more processors, cause said set of processors to perform operations comprising:

without proxying, analyzing each of a stream of packets traversing a single connection through the network access device from an external host to a protected host;

forwarding each allowed packet of the stream of packets as long as the connection is active; and

if one of the stream of packets is determined to be disallowed by said analyzing, then discarding the disallowed packet and terminating the connection, causing the protected host to discard those packets received on the terminated connection.

29. The machine-readable medium of claim 28 wherein analyzing each of the stream of packets comprises inspecting a header of each of the stream of packets against a packet filter.

30. The machine-readable medium of claim 28 wherein analyzing each of the stream of packets comprises inspecting a payload of each of the stream of packets for disallowed content.

31. The machine-readable medium of claim 30 wherein inspecting the payload of each of the stream of packets comprises copying the payload, analyzing the payload, and discarding the corresponding packet if the payload is threatening.

32. The machine-readable medium of claim 28 further comprising:

copying a payload from each of a plurality of packets that comprise a file, the stream of packets including the plurality of packets;

forwarding all but the last of the plurality of packets to the protected host;

reassembling the plurality of packets into the file;

analyzing the file;

if the file is a threatening file then discarding the last packet and terminating the connection; and

if the file is non-threatening, then forwarding the last packet.

33. A machine-readable medium that provides instructions, which when executed by a set of one or more processors, cause said set of processors to perform operations comprising:

copying a packet payload of each of a plurality of packets received on a single connection between an external host and a protected host that carries a stream of packets the stream of packets including the plurality of packets;

forwarding all but the last of the plurality of packets to the protected host;

reassembling the copied packet payloads into a file;

analyzing the file to determine if the file is allowed or disallowed;

if the file is allowed, then forwarding the last packet to the protected host; and

if the file is determined to be disallowed, then dropping the last packet and terminating the connection.

34. The machine-readable medium of claim 33 wherein the analyzing the file comprises performing anti-virus analysis on the file.

35. The machine-readable medium of claim 33 further comprising:

analyzing a header of each of the stream of packets; and

if one of the stream of packets is determined to be disallowed, then discarding the disallowed packet and terminating the connection.

36. The machine-readable medium of claim 35 wherein analyzing the header comprises inspecting addresses indicated in the header against a packet filter.

37. The machine-readable medium of claim 33 further comprising:

individually analyzing each of the copied packet payloads; and

if one of the copied packet payloads is determined to be threatening, then discarding the corresponding packet and terminating the connection.

38. The machine-readable medium of claim 37 wherein analyzing each of the copied packet payloads comprises inspecting each copied packet payload against a list of disallowed content and determining if each copied packet payload includes threatening script.

39. The machine-readable medium of claim 33 further comprising maintaining the connection while analyzing the file.

40. The machine-readable medium of claim 39 wherein maintaining the connection comprises:

decapsulating the last packet's payload;

fragmenting the last packet's payload into subparts;

encapsulating each subpart; and

forwarding each subpart until analysis is complete.

41. The machine-readable medium of claim 39 wherein maintaining the connection comprises:

copying each of the plurality of packets but the last packet before forwarding each of the plurality of packets; and

holding the last packet and repeatedly forwarding the last copied packet.

42. The machine-readable medium of claim 39 wherein maintaining the connection comprises increasing transmission latency of each acknowledgement transmitted from the protected host to the external host until the analysis is complete.

43. The machine-readable medium of claim 33 wherein forwarding each of the plurality of packets comprises transmitting a message indicating that each of the of the plurality of packets is allowed.

44. A machine-readable medium that provides instructions, which when executed by a set of one or more processors, cause said set of processors to perform operations comprising:

supporting a connection from an external host to a protected host;

analyzing a header of each packet received over the connection from the external host;

terminating the connection if a first packet received over the connection is determined to be disallowed and discarding the first packet;

if the connection is not terminated, copying the first packet's payload;

analyzing the first packet's payload;

terminating the connection if said first packet's payload is determined to be disallowed and discarding the first packet;

if the connection has not been terminated and if said first packet's payload is not a last block of a file, then forwarding said first packet to the protected host;

if said first packet's payload is the last block of a file, then reassembling the first packet's payload with a set of one or more previously copied packet payloads into the file;

analyzing the file to determine if the file is allowed or disallowed;

if the file is disallowed then dropping the first packet and terminating the connection; and

if the file is allowed then forwarding the first packet.

45. The machine-readable medium of claim 44 further comprising maintaining the connection while analyzing the file.

46. The machine-readable medium of claim 45 wherein maintaining the connection comprises:

decapsulating the last packet's payload;

fragmenting the last packet's payload into subparts;

encapsulating each subpart; and

forwarding each subpart until analysis is complete.

47. The machine-readable medium of claim 45 wherein maintaining the connection comprises:

copying each of the plurality of packets but the last packet before forwarding each of the plurality of packets; and

holding the last packet and repeatedly forwarding the last copied packet.

48. The machine-readable medium of claim 45 wherein maintaining the connection comprises increasing transmission latency of each acknowledgement transmitted from the protected host to the external host until the analysis is complete.

49. The machine-readable medium of claim 33 wherein the analyzing the file comprises performing anti-virus analysis on the file.

50. The machine-readable medium of claim 35 wherein analyzing the header comprises inspecting addresses indicated in the header against a packet filter.

51. The machine-readable medium of claim 37 wherein analyzing each of the copied packet payloads comprises inspecting each copied packet payload against a list of disallowed content and determining if each copied packet payload includes threatening script.